REMARKS

In the Official Action mailed on **11 March 2009**, the Examiner reviewed claims 1-22. Examiner objected to claim 8 because of informalities. Examiner rejected claims 9 and 16 under 35 U.S.C. § 112. Examiner rejected claims 8-22 under 35 U.S.C. § 103(a) based on Porras et al. (U.S. Pub. No. 2004/0010718, hereinafter "Porras"), and Pruthi et al. (U.S. Patent No. 7,492,720, hereinafter "Pruthi"). Examiner rejected claims 1-7 under 35 U.S.C. § 103(a) based on Porras, Pruthi, and Cooper et al. (U.S. Patent No. 7,047,288, hereinafter "Cooper").

Objections to the Claims

Examiner objected to claim 8 because of informalities. Specifically, Examiner objected to claim 8 because it recites "longer duration that a current period." Applicant has amended claim 8 so that "that a" now reads "than a."

Rejections under 35 U.S.C. § 112

Examiner rejected claims 9 and 16 under 35 U.S.C. § 112. Specifically, Examiner stated that the phrase "determine if the host is providing or using the new service" is unclear. Applicant has amended these claims so that they now include the limitation "determine if the host is **sending traffic using a protocol not in the current list** or **receiving traffic with a protocol not in the current list**. Support for these amendments is found in instant application, P16:L6-10, P16:L29-P17:L11. No new matter has been added.

Rejections under 35 U.S.C. § 103

Examiner rejected claims 1-7 as being unpatentable over Porras, in view of Pruthi and Cooper. Examiner rejected claims 8-22 under as being unpatentable over Porras in view of Pruthi. Applicant respectfully disagrees with these rejections. Neither Porras, Pruthi, nor Cooper distinguishes between hosts that are **providing** a new service and hosts that are **using or consuming** the new service.

Porras discloses monitoring network packets, building statistical profiles derived from network packets, and determining if the statistical profile is anomalous (Porras, Fig. 4). Note that the statistical analysis in Porras (Porras, par. [0035]) is not collected over every host pair as in embodiments of the present invention. Furthermore, Porras discloses that the statistical analysis can be based on event records can be derived from discarded traffic (i.e., packets not allowed through the gateway because they violate filtering rules), pass-through traffic (i.e., packets allowed into the internal network from external sources), packets having a common protocol, packets that reach the gateway, packets involving network connection management, and packets targeting ports to which an administrator has not assigned any network service and that also remain unblocked by the firewall (Porras, par. [0033]).

Note that selection in Porras, which is based on targeting a particular network service or application, does **not** enable the Porras system to distinguish between hosts that are **providing** a new service and hosts that are **using or consuming** the new service.

Pruthi similarly discloses collecting statistics at the **packet level**, specifically:

> …byte counts, bit counts, one-way or roundtrip delays, response times, retransmitted bytes, originating bytes per host, terminating bytes per host, originating-terminating host pair counts, web abort rates, throughput,

goodput, and percent retransmitted bytes due to delays or losses (Pruthi, C4:L36-41).

Nowhere does Pruthi disclose distinguishing between hosts that are **providing** a new service and hosts that are **using or consuming** the new service.

Cooper discloses a graphical user interface for specifying a host name and the type of service being tracked (Cooper, Figs. 9 and 31). However, Cooper does not disclose a graphical user interface to facilitate distinguishing between hosts that are **providing** a new service and hosts that are **using or consuming** the new service.

In contrast, embodiments of the present invention involve distinguishing between hosts that are **providing** a new service and hosts that are **using or consuming** the new service (instant application, FIG. 10: elements 104, 106, and 108). By distinguishing between hosts that are providing a new service and hosts that are using or consuming the new service, the system can better distinguish the origin of an attack.

Nothing within Porras, Pruthi, and Cooper, either separately or in concert, suggests or implies distinguishing between hosts that are **providing** a new service and hosts that are **using or consuming** the new service.

Applicant has amendment independent claims 1, 8, and 15 to clarify that embodiments of the present invention involve distinguishing between hosts that are **providing** a new service and hosts that are **using or consuming** the new service. In response to a suggestion by Examiner during a 12 May 2009 phone conversation with Examiner:

- Applicant has amended claims 1-7 to clarify that embodiments of the present invention involve computer systems configured to display a graphical user interface for configuring a new service alert rule.
- Applicant has amended claim 8 to clarify that issuing an alert is based at least on the identified alert rule and whether the host is providing or using the new service.

Support for these amendments is found in instant application, FIG. 10: elements 104, 106, and 108, and par. [0026]. Applicant has cancelled claims 10 and 17 and amended claims 11 and 19 to ensure proper claim dependency. No new matter has been added.

Hence, Applicant respectfully submits that independent claims 1, 8, and 15 as presently amended are in condition for allowance. Applicant also submits that claims 2-7, which depend upon claim 1, claims 9 and 11-14, which depend upon claim 8, and claims 16 and 18-22, which depend upon claim 15, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By /Shun Yao/
Shun Yao
Registration No. 59,242

Date: 13 July 2009

Shun Yao
Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
Fax: (530) 759-1665
Email: shun@parklegal.com